

Altiris™ Monitor Solution for Servers 7.1 SP2 and Event Console 7.1 SP2 from Symantec™ Release Notes



Altiris™ Monitor Solution for Servers 7.1 SP2 and Event Console 7.1 SP2 from Symantec™ Release Notes

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Legal Notice

Copyright © 2011 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, Altiris, and any Altiris or Symantec trademarks used in the product are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
<http://www.symantec.com>

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
 - Error messages and log files
 - Troubleshooting that was performed before contacting Symantec
 - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Altiris™ Monitor Solution for Servers 7.1 SP2 and Event Console 7.1 SP2 from Symantec™ Release Notes

This document includes the following topics:

- [About Altiris™ Monitor Solution 7.1 SP2 and Event Console 7.1 SP2](#)
- [What's new in this version](#)
- [General installation and upgrade information](#)
- [Known issues](#)
- [Fixed issues](#)
- [Other things to know](#)
- [Documentation that is installed](#)
- [Other information](#)

About Altiris™ Monitor Solution 7.1 SP2 and Event Console 7.1 SP2

Monitor Solution helps you ensure your server uptime and availability, and it ultimately reduces the costs of network management in your organization.

Monitor Solution lets you accomplish the following tasks:

- Identify the health of your environment by collecting detailed data from servers, applications, and network devices.
- Analyze trends and isolate recurring issues by collecting comprehensive real-time and historical performance data.
- Pinpoint problems, define their cause, and take automated actions to resolve them.

Event Console reduces the need to maintain separate tools to monitor computers, software, printers, and other devices. Event Console collects SNMP traps and other status messages and displays them in a single location. If the originator of the alert is a resource in the database, all status messages that Event Console receives are converted to a common format. Each formatted message that is received is linked to the affected resource in the Configuration Management Database (CMDB). These formatted messages are called alerts.

These products are part of the following suites:

- Altiris™ Client Management Suite from Symantec™ (Event Console only)
- Altiris™ Server Management Suite from Symantec™
- Altiris™ IT Management Suite from Symantec™

What's new in this version

In the 7.1 SP2 release of Monitor Solution, the following new features are introduced:

Table 1-1 List of new features in Monitor Solution

Feature	Description
Support for new platforms.	You can install Monitor Agents on the computers that are running the following platforms: ■ Red Hat Enterprise Linux 6.0 x86/x64 ■ Red Hat Enterprise Linux 6.1 x86/x64 ■ SUSE Linux Enterprise Server 11 SP1 x86/x64 ■ Solaris 10 Update 7

Table 1-1 List of new features in Monitor Solution (*continued*)

Feature	Description
Changes on the Monitoring and Alerting Portal page.	The following changes were made on the Monitoring and Alerting Portal page: ■ The Activated Monitor Policies Web part was removed. Note that the Web part is still available under Settings > Notification Server > Console Settings > Web Parts > Monitoring. ■ Monitor Site Servers Status Web part was added. ■ Group View - Aggregate health by resource Web part was added.

The 7.1 SP2 release of Event Console includes enhancements to refine product quality.

General installation and upgrade information

You install this product by using the Symantec Installation Manager. You can download the installation files directly to your server or you can create offline installation packages.

For more information, see the *Installing IT Management Suite* chapter in the *IT Management Suite 7.1 SP2 Planning and Implementation Guide* at the following URL:

<http://www.symantec.com/docs/DOC4827>

See the product's documentation for information on how to configure and use it.

To perform an upgrade from version 7.1 or later, in the Symantec Installation Manager click **Install New Products**, and then choose to install this product. Do not use the **Install Product Updates** page to upgrade.

Symantec recommends that you upgrade all of the installed products to the latest version. The easiest way to achieve this is to choose to install a suite.

If you use hierarchy, you must disable hierarchy replication and upgrade all products to the latest version on each of the Notification Server computers.

For additional information about upgrading, see the **Upgrading to IT Management Suite 7.1 SP2 - Best Practices** article at the following URL:

<http://www.symantec.com/docs/TECH177513>

After you upgrade the product, you must upgrade the Symantec Management Agent and the plug-ins that are installed on the managed computers. Symantec recommends that you do the following:

- In the Symantec Management Console, click **Actions > Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, under **Symantec Management Agent**, locate and turn on the upgrade policies for the Symantec Management Agent.
- In the Symantec Management Console, click **Settings > All Settings**. In the left pane, expand **Notification Server > Site Server Settings**, and then locate and turn on the upgrade policies for various site server plug-ins.
- In the Symantec Management Console, click **Actions > Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, locate and turn on the upgrade policies for various plug-ins.

Symantec recommends that you configure a schedule for these policies; the default **Run once ASAP** option may not trigger the policy if this is not the first time you perform an upgrade. Also, to speed up the upgrade process, consider temporarily changing the **Download new configuration every** setting on the **Targeted Agent Settings** page to a lower value.

For detailed instructions on migrating from 6.x and 7.0 to 7.1 SP2, see the following documentation resources:

- *IT Management Suite Migration Guide version 6.x to 7.1 SP2* at the following URL:
<http://www.symantec.com/docs/DOC4742>
- *IT Management Suite Migration Guide version 7.0 to 7.1 SP2* at the following URL:
<http://www.symantec.com/docs/DOC4743>

Known issues

The following are known issues for this release. If additional information about an issue is available, the issue has a corresponding Article link.

The known issues are separated into the following components:

- Monitor Solution
[Table 1-2](#)
- Event Console
[Table 1-3](#)

Table 1-2 Known issues for Monitor Solution

Issue	Description	Article Link
After upgrade the Remote Monitor Server becomes uninstalled.	After completing the upgrade from IT Management Suite 7.1 MP1 to IT Management Suite 7.1 SP2 the Remote Monitor Server x86 and Remote Monitor Server x64 automatically become uninstalled.	
Uninstalling Monitor Solution does not remove all its items.	When you uninstall Monitor Solution, some of the Monitor Solution related tasks (for example, Monitor License status and Monitor Purge item) remain on the server and continue working.	
The Create a monitor policy wizard stops responding.	The Create a monitor policy wizard stops responding if in the Choose what to monitor panel, you click Next or Finish without entering a name for the policy.	
The Custom DLL Metric does not work with DLL files compiled on a 64-bit computer.	The Custom DLL Metric page only works with the DLL files that were compiled on a 32-bit computer. If a specified DLL file was compiled on a 64-bit computer, an error message is sent. The state of the metric also changes to Retry State.	TECH153171
Details of forwarded alerts are not displayed correctly on the Management Station console.	After you add and save a new rule, and then send alerts based on the rule, the categories Hostname, Definition, and Protocol are not displayed correctly on the Management Station console.	
Customized Monitor rollout policy targets are rewritten with default values during upgrade.	When you upgrade to Monitor Solution 7.1 from 7.0 SP4 HF1, all customized targets for the Monitor Plug-in rollout policies are rewritten with default values.	
You cannot change some NT Event Task settings.	If you try to change some NT Event Task settings (Event Source, Category ID, Event ID), they are not saved. They are only saved if Event Source Name is changed as well.	
Incorrect heartbeat alert behavior on a virtual machine.	A heartbeat alert may be raised in Event Console from a monitored resource that runs on a virtual machine, even if it is online and the metric provider is running.	
Monitor token values that include double quotes cause VBScript tasks to fail.	If you have a VBScript client side task that is associated with a rule and the output from a token produces double quotes, the VBScript fails.	TECH154599
The Disk Paging Activity report displays incomplete data.	The Disk Paging Activity report displays incomplete HP-UX and AIX data when it is viewed in the Chart View.	

Table 1-2 Known issues for Monitor Solution (*continued*)

Issue	Description	Article Link
Agentless monitoring uses Pluggable Protocol Architecture (PPA) connection profiles.	The Remote Monitoring Server (RMS) agent leverages PPA to make connections to monitored remote resources to obtain metric data. PPA references the connection profiles used during Network Discovery. The Network Discovery Connection Profiles define which protocols are enabled and any applicable credentials and settings for each protocol. When the RMS agent attempts to monitor an agentless resource, it queries the database and uses the connection profile that was used during Network Discovery. If the RMS agent cannot find a reference to a connection profile, the Default connection profile is used. To select a different connection profile, run a new Network Discovery and select the desired connection profile for remote resources.	
Unable to assign a connection profile to a resource.	On the Manage Connection Profile page, when you create connection profiles for different configured clients, the user is not able to assign (to map) connection profiles to the resources.	
WS-Management service cannot process the request on Windows clients.	WS-Management service does not work on Windows clients because it cannot process the request. The service cannot find the resource that the resource URL and selector identify.	
Limited monitoring of ESX Servers.	Monitoring of ESX Servers is limited when using the WS-MAN Agentless metric because of limitations in Pluggable Protocol Architecture (PPA).	
Time drifting issues occur when monitoring heartbeats on Linux computers that are hosted on VMware.	When monitoring heartbeats on Linux computers that are hosted on VMware, there are issues with time drifting. This issue can cause Notification Server to receive heartbeats after a very long delay and an alert to be raised in the Event Console. To avoid issues with unnecessary alerts in the Event Console, make sure that your heartbeat time settings are synchronized to account for possible time drifting.	

Table 1-2 Known issues for Monitor Solution (*continued*)

Issue	Description	Article Link
The Poll Metric on Demand task cannot poll agent-based metrics on a computer that does not have the Monitor Plug-in.	The Poll metric on demand task can poll two different types of metrics: agent-based and agentless. It is supported on two different types of targets: with and without Monitor Plug-in. If the Poll metric on demand Task is executed on an agentless target without the Monitor Plug-in installed, then it can only poll agentless metrics on that computer. Agent-based metrics are not polled on an agentless client computer as agent-based metrics require the Monitor Plug-in to run.	
Network Discovery found devices may not be listed in the targeted filters of the default agentless policy.	Agentless monitor policies target filters of computers and devices. By default, the target includes only unmanaged devices running Windows 2003 or 2008. When computers are discovered, the local operating system is a property of that computer resource. If during discovery, a computer's operating system cannot be determined, an operating system-specific filter does not recognize that computer. If an agentless monitor policy is not running on a computer as expected this issue is a possible cause. Note: The operating system version is correctly discovered for the target computers that have SNMP enabled.	
A failed heartbeat may not raise an alert if the Check for heartbeat every option is less than the Send heartbeat every option with zero retry attempts.	A failed heartbeat may not raise an alert in the Event Console due to network latency when you have the following configuration: ■ The Retry every option on the Heartbeat tab of the Monitor Server Settings page has a value of "0". ■ The value of the Check for heartbeats every option is less than or equal to the Send heartbeat every option on the Data Collection tab of the Monitor Plug-in Configuration Settings page. In this case, a Monitor Plug-in may appear to occasionally go down only to come right back up again. However, the uptime data is not affected in this case.	

Table 1-2 Known issues for Monitor Solution (*continued*)

Issue	Description	Article Link
Agentless monitoring is not available for the targets that have been discovered through an Active Directory Import.	You cannot apply agentless monitor policies to targets that have been discovered through an Active Directory Import. Workaround: Use a Network Discovery or a WINS import instead of an Active Directory Import.	
You must reconnect the Real-time Performance Viewer if metric data becomes unavailable.	When you use the Real-time Performance Viewer, if a metric becomes unavailable and then becomes available again, updated data is not displayed. The viewer continues to display the data value that was last received before the metric became unavailable. The Real-time Performance Viewer must be re-connected to the target computer before updated data is reflected in the viewer.	
Monitor RMS 7.0.2671 RMS cannot get information for HTTP metrics from password-protected resources.	In some cases Monitor RMS 7.0.2671 RMS cannot get information for HTTP metrics from password-protected resources.	
There is a delay in the Computers List for the Real-time Viewer and Historical Performance Viewer.	Computers are not populated in the Computers List for the Real-time Viewer and Historical Performance Viewer until data is received from the target computer by Notification Server.	
A customized view of a Monitor Solution report is not preserved after the report refreshes.	After you customize the view of a Monitor Solution report, the customizations to the view are lost when the report is refreshed. The report then displays the default view.	
When "Altiris" log type is selected, the Log Event metric only supports Windows platforms.	When the "Altiris" log type is selected, the Log Event metric uses Notification Server log file as source. This type of log is supported for Windows platforms only.	
HTTP metrics do not support virtual hosts.	The HTTP metric cannot be used with virtual hosting. The HTTP metric only supports the use of the current host name of a physical computer that reports basic inventory to the Notification Server computer.	TECH40807

Table 1-2 Known issues for Monitor Solution (*continued*)

Issue	Description	Article Link
An error occurs when you export a monitor pack to Windows Vista and Windows Server 2008 with active IE protected mode.	The monitor pack's .XML file is copied to the \temp\ folder instead of the intended path. In this case, completing the import process from this location would fail. This error occurs when you export a monitor pack to a Windows Vista or a Windows Server 2008 computer with Internet Explorer protected mode ON.	
WMI metrics read the data with the lowest polling interval.	If two WMI metrics are configured to parse the same command output and they both have different polling intervals, these metrics read the data with the lowest polling interval. The WMI metrics combine into a similar query for optimization. The query runs at the lowest interval setting.	
Unable to get monitor Data from Linux client.	You cannot get monitor data from Linux client due to port 1011 closed. An error <i>Error Retrieving Metrics</i> appears.	TECH154964
Metrics do not work if Credential Manager is installed by pull to Remote Monitor Server.	Some metrics do not work if Credential Manager is installed by a pull to the Remote Monitor Server. If Credential Manager is pushed to the Remote Monitor Server, there are no problems.	See cause A in TECH121926 .
Polling metric on demand task fails.	If you add the Poll metric on demand task to a policy or to a rule, then the task fails to run when the rule is activated. The task completes successfully when manually executed.	

Table 1-3 Known issues for Event Console

Issue	Description	Article Link
It is not possible to export or import Alert Rule Settings from Event Console .	It is not possible to export and import Alert Rule Settings from the Event Console page. Workaround: On a source server, do the following: ■ In the Symantec Management Console, on the Settings menu, click Monitoring and Alerting. ■ In the left pane, expand Event Console, and click Alert Rule Settings. ■ In the right pane, right-click each rule, and then click Export. ■ Save the rules. On a target server, do the following: ■ In the Symantec Management Console, on the Settings menu, click Monitoring and Alerting. ■ In the left pane, expand Event Console, and click Alert Rule Settings. ■ In the right pane, right-click on any item in the list, and then click Import. ■ Select the previously saved rules.	
Email is received without information about alert variable.	User cannot configure email task to view alert variable in the email subject.	TECH154601
Event Console page refreshes every hour.	When the Event Console page refreshes, it resets the filter to the default value. The Event Console page is refreshed every hour to prevent memory leak.	
Unable to delete a task rule after a task is changed.	On the Task Rules tab of the Alert Rule Settings page, if a task in a task rule is changed, you then cannot delete the task rule.	TECH154422
Event Console Web part does not appear.	The Event Console Web part should appear on the Resource Manager Portal page that is accessed from the Home menu of Resource Manager. However, the Event Console Web part currently does not display. You must contact support for a point fix to resolve this issue.	

Table 1-3 Known issues for Event Console (*continued*)

Issue	Description	Article Link
The Acknowledge and Resolve options become disabled in some cases.	When you select multiple alerts holding down the Shift key, the Acknowledge and Resolve options on the toolbar become unavailable. Workaround: Right-click any of the selected items and click Acknowledge or Resolve.	

Fixed issues

The following are the fixed issues in this release. If additional information about an issue is available, the issue has a corresponding Article link.

The fixed issues are separated into the following components:

- Monitor Solution

[Table 1-4](#)

- Event Console

[Table 1-5](#)

Table 1-4 Fixed issues for Monitor Solution

Issue	Description	Article Link
	In some cases, the Remote Monitor Server stops responding.	
	Monitor Plug-in stops responding when processing NT Events that are generated by a custom application.	
Slow performance of the metric list retrieving data from the monitored resources.	Performance of the metric list retrieving data from the Windows Agent-based monitored resources is slow. It can take up to 2 minutes to retrieve the data.	
Monitor Plug-in stops functioning.	When you upgrade Monitor Solution but do not upgrade the Monitor Plug-in, the Monitor Plug-in stops functioning.	
Monitor Plug-in upgrade can get installed on a non-supported operating system when the default target is used.	When you upgrade from Monitor Solution 7.0 SP5 to 7.1 MR1, the Monitor Plug-in upgrade policy installs the Monitor Plug-in on Windows 2003 SP1. Because Windows 2003 SP1 is not supported for the Monitor Plug-in, it does not work. When upgrading the Monitor Plug-in, use a custom target that does not include Windows 2003 SP1.	

Table 1-4 Fixed issues for Monitor Solution (continued)

Issue	Description	Article Link
Log Event metric fails to monitor the folder on UNIX/Linux.	When you configure a Log Event metric to monitor all logs in a folder at a custom location, the metric does not work, the data is not collected, and the metric rule does not trigger.	
A memory leak is in "Win32_Service" WMI class for Windows 2008 R2.	When you use "Windows Service" metric that uses "Win32_Service" WMI class on Windows Server 2008 R2, you may see HEAP usage % increase using the Microsoft Utility 'dheapmon'. Microsoft has already fixed this issue. For more information, see: http://www.support.microsoft.com/kb/981314	

Table 1-5 Fixed issues for Event Console

Issue	Description	Article Link
Event Console Alert Rule does not function.	Event Console Alert Rule does not function if you enter an IP address for a if Alert hostname (or IP) clause.	
	The Event Console Alert Rule value field does not function properly when you try to enter or paste text.	

Other things to know

The following are things to know about this release. If additional information about an item is available, the item has a corresponding Article link.

The other things to know are separated into the following components:

- Monitor Solution
[Table 1-6](#)
- Event Console
[Table 1-7](#)

Table 1-6 Other things to know about Monitor Solution

Items	Description	Article Link
You may need to install sysstat on your monitored Linux computers.	You must install sysstat on your targeted Linux computers to use the following monitor policies: ■ Processor ■ Disk I/O ■ Memory ■ Linux Server Health	
The repeat count feature specifies the number of times the rule must trigger in a row before an action is taken.	After the repeat count specified in a rule has been reached, the rule resets to "normal" on the next value, even if that value crosses the threshold. If the value crosses the threshold, the rule restarts the repeat count for the next evaluation. Example: Rule count definition - if CPU > 10 for three times. If the values are 11, 12, 13, 11, the rule triggers on the third value and then resets to normal on the fourth value. Note: Repeat count for rule increases for each condition which is met instead of for the overall criteria for the rule.	
Activated Monitor Policies Web part only shows the policies that the Monitor Plug-in has activated.	The Monitor Plug-in must first activate a monitor policy before it is displayed in the Activated Monitor Policies Web part of the Monitoring and Alerting home page. If you enabled a monitor policy but it is not yet displayed in the Web part, it might be because the Web part is populated from inventory data that is received from the plug-in.	

Table 1-6 Other things to know about Monitor Solution (*continued*)

Items	Description	Article Link
Purging Log Event and Sys Log data.	Both Log Event and Sys Log data purging is controlled with the single String metric data purging schedule. To schedule string metric data purging: 1 In the Symantec Management Console, on the Home menu, click Monitoring and Alerting. 2 In the left pane, click Monitoring and Alerting > Monitor > Settings > Monitor Server Settings. 3 On the Monitor Server Settings page, click the Purge Maintenance tab. 4 Under Non-numeric Data, set the value for String metric data. 5 On the Monitor Server Settings page, click Save changes.	
The specific setup is required to enable Smart Metrics using SNMP.	To enable Smart Metrics using SNMP: ■ The SNMP service must be installed on the monitored computer. ■ The community name must be configured in the SNMP service on the monitored computer. The community name must match the community string in the SNMP protocol settings for your connection profile. ■ SNMP packets must be accepted from any host in the SNMP properties on the monitored computer.	
How WMI Metric handles WMI property arrays.	In some cases WMI property values are stored as arrays of values. In this case, each property in the array is represented as a different instance\value pair for the metric. The name for instance is "Name of the instance (n)" where n is the index. For example, if % Disk Space had multiple properties for disk space: "C: (1)" = 23, "C: (2)" = 43, "D: (1)" = 54, "D: (2)" = 7	

Table 1-7 Other things to know about Event Console

Items	Description	Article Link
New condition types are added to the Event Console alert rules.	The starts with and ends with condition types are added to Event Console alert rules.	

Table 1-7 Other things to know about Event Console (*continued*)

Items	Description	Article Link
Help is not available on the Workflow rule tab.	On the Workflow rule tab of the Alert Rule Settings page, the context-sensitive help may not appear when you click F1. To display the context-sensitive help for the Workflow rule tab, you must first create a workflow rule and click on the Web part that contains the rule before clicking F1.	

Documentation that is installed

Table 1-8 Documentation that is included in the product installation

Document	Description	Location
Help	Information about how to use this product. Help is available at the solution level and at the suite level. This information is available in HTML help format.	The Documentation Library, which is available in the Symantec Management Console on the Help menu. Context-sensitive help is available for most screens in the Symantec Management Console. To open context-sensitive help, click inside the window, pane, dialog box, or other screen element about which you want more information, and then do one of the following: ■ Press the F1 key. ■ In the Symantec Management Console, click Help > Context. In the Symantec Help Center window, type your search string to search within the installed documentation. To expand your search to the Symantec Knowledge Base, check Include online search. For more information on how to use the Symantec Help Center, click the Home symbol.
User Guide	Information about how to use this product. This information is available in PDF format.	■ The Documentation Library, which is available in the Symantec Management Console on the Help menu. The Documentation Library provides a link to the PDF User Guide on the Symantec support Web site. ■ The Supported Products A-Z page, which is available at the following URL: http://www.symantec.com/business/support/index?page=products Open your product's support page, and then under Common Topics, click Documentation.

Other information

Table 1-9 Information resources that you can use to get more information

Document	Description	Location
<i>ITMS 7.1 SP2 Planning and Implementation Guide</i>	Information about capacity recommendations, design models, scenarios, test results, and optimization best practices to consider when planning or customizing ITMS.	http://www.symantec.com/docs/DOC4827
<i>Symantec Management Platform User Guide</i>	Information about using the Symantec Management Platform.	Symantec Management Platform Documentation page
<i>Symantec Management Platform Release Notes</i>	Information about new features and important issues in the Symantec Management Platform.	Symantec Management Platform Documentation page
<i>Symantec Management Platform Installation Guide</i>	Information about using Symantec Installation Manager to install the Symantec Management Platform products.	http://www.symantec.com/docs/DOC4798
Knowledge base	Articles, incidents, and issues about this product.	SymWISE support page
Symantec Connect	An online magazine that contains best practices, tips, tricks, and articles for users of this product.	Symantec Connect page